**Reflection Report Guidelines**

By:

Oluwabunmi Olanrewaju

Contents

[Ethical Decision Making Cases 3](#_Toc6230783)

[Case 1: **Ethical Decision Making in Information Technology** 3](#_Toc6230784)

[Case 2: **Ethical Decision Making in Information Technology (A case study of Security Breach)** 11](#_Toc6230801)

[Speaker Reflection 22](#_Toc6230802)

[Speaker 1: Matthew Vaughan /SGI 22](#_Toc6230803)

[Speaker 2: Todd Anthill / Nutrien 23](#_Toc6230810)

[Speaker 3: **2nd Year BIS Volunteers** / COOP Student Panel 24](#_Toc6230816)

[Speaker 4: Mark Plosz / Paradigm Consulting 25](#_Toc6230822)

[Appendices 26](#_Toc6230828)

[Appendix A. Ethical Decision Making Framework 26](#_Toc6230829)

[Appendix B. Speaker Feedback Emails 27](#_Toc6230830)

# Ethical Decision Making Cases

## Case 1: **Ethical Decision Making in Information Technology**

**Ethical Decision Making in Information Technology**

**(COMP 249-001 - Info Security, Privacy and Ethic)**

**Group Members:**

Anuka, Munachi

Olanrewaju, Oluwabunmi

# Why do IT professionals need a code of ethics?

## What is ethics?

Ethics may be considered as regulations which differentiate between right and wrong. It also aims to differentiate between acceptable and unacceptable behaviour.

## What is Code of Ethics?

 A code of ethics is a document that outlines a set of acceptable behaviors for a professional or social group

## Why do professionals in general create codes of ethics to govern their behaviour

* **Work Place**

Professionalism is the key work for all businesses in order to provide the best quality service to their customers which in turns increase profits, productivity among employees and market value in their respective sectors. To achieve this professionalism, it is necessary to create codes of ethics to govern employees and the codes covers trustworthiness, responsibility, punctuality, confidentiality, team player, competency and good reputation. In summary, ethics help:

* Attract customers to the firm’s products, which means boosting sales and profits
* Make employees want to stay with the business, reduce labour turnover and therefore increase productivity
* Attract more employees wanting to work for the business, reduce recruitment costs and enable the company to get the most talented employees
* Attract investors and keep the company’s share price high, thereby protecting the business from takeover.
* Risk Mitigation
* **Around their profession**

Professional ethics establishes a baseline for common decency, respect, fairness, and integrity in given business area and it is necessary for the following reasons:

* It ensures accountability as it provides guidelines and ways of identifying moral hazards and providing the appropriate avoidance or work-around strategies.
* Professional ethics represents a kind of collective, time-tested wisdom that is passed on to new individuals in the profession. Also with changing laws, technologies and mores, professional standards will work to keep the profession abreast of new ethical challenges and emerging responsibilities and best practices.
* professional ethics often get promulgated by professional organizations, they may play a role in enforcement and disciplinary action with respect to those who violate such standards.
* **How they relate to those they serve**
* to the public, as they build confidence in the profession’s trustworthiness
* clients, as they provide greater transparency and certainty about how their affairs will be handled
* members of the profession, as they provide a supporting framework for resisting pressure to act inappropriately, and for making acceptable decisions in what may be ‘grey areas’
* the profession as a whole, as they provide a common understanding of acceptable practice which builds collegiality and allows for fairer disciplinary procedures
* others dealing with the profession, as the profession will be seen as more reliable and easier to deal with.

## How do ethics apply to IT professionals?

Since technology can be used as a benefit or for destruction, ethics play a major role in determining the right use of technology. IT professional must have proper code of conduct, right attitude and good moral values and should not misuse the technology.

Nowadays, due to the rapid advancement in technology there has been a widespread misuse of technology. With the rise of Internet there has been unethical and unprofessional behaviour which have led to severe problems such as computer viruses, Spamming, cybercrimes and hacking. Everyone in the IT must be made aware of the consequences which result due to unethical behavior and this must be taught at the early stage such as teaching a student. Professionalism must be strictly followed from schools and institutions and should be practiced at an earlier stage.

## Areas where IT decision making could have ethical implications

**Security:** The main essence of security in IT is to maintain integrity and confidentiality of sensitive information and prevent access of such information by hackers. IT security helps ensure only authorized users access and make changes to sensitive information. So, it is necessary for an IT personnel to provide adequate processes and tools to prevent malicious threats and potential security breaches that can have a huge impact on your organization.

**Copyright Infringement**:  It is easy nowadays for people to access any information especially online.  For instance, there is increased development of music sharing networks, many original creators of these works are losing the credibility of their works, because users of IT can easily gain access and share that data with friends. Free music and file downloading sites are popping up on internet every day, lots of original work like music albums, books, are being downloaded for free. In this case, one legitimate user will purchase the book, software, web template or music album, and they will submit it to a free download site where others will simply just download that data for free. It is good news for the users because it saves them money, but it harms the original creator of these works. There is also a situation of Plagiarism; Plagiarism is where the work of others is copied, but the author presents it as his or her own work. This is a highly unethical practice

**MALICIOUS CODES:** Malicious code attacks include a number of types of computer programs that were created with the intention of causing data loss or damage. The three main types of malicious code attacks are viruses, Trojan horses, and worms. Clearly writing and spreading virus programs are unethical acts; they have very serious consequences, and cause systems to crash and organisations to cease operating for certain periods. One of the most concerning consequences of such actions is when viruses interrupt the smooth functioning of an organization.

**Privacy:** Organisation should be responsible for any information collected from clients/customers

# Deontological vs. Teleological views of Ethics

**Deontological ethics** also known as “duty-based” ethics, it state right action consists in following our duty, irrespective of the consequences while **Teleological ethics** (also called [consequentialism](http://en.wikipedia.org/wiki/Consequentialism)) focus actual consequences of an action, as that which makes an action praiseworthy or blameworthy.

## Scenario Analysis

**Deontological and Teleological implications**

Using deontological ethics, the grocery store chain is duty-bound not to use customer data to track and warm people that they have purchased an unsafe product; as the main essence of the loyalty program database is to help the grocery store with their supply chain management and to help the grocery plan sales and promotions. Using it for any other purpose will result to invasion of privacy which is not unethical.

on the other hand, using teleological ethics, it will be morally right to inform the customers of their purchased of an unsafe product which is harmful to their health although it might be invasion of privacy but at the end, the action is praiseworthy.

**After these considerations what would you do?**

We will go with Teleological ethics, base on the fact that using the information is for a greater good in comparison to the invasion of privacy which most customers will appreciate.

Also, not informing the customers might lead to lawsuits between customers and *grocery store chain* as the harmful products were gotten from the store. The lawsuit might eventually lead to greater loss in comparison to not using the information.

# A Frame Work for ethical problem solving

Making good ethical decisions requires a understanding ethical issues and a practiced method for exploring the ethical aspects of a decision and weighing the considerations that should impact our choice of a course of action. Having a method for ethical decision making is essential and it involves the following steps:

**Recognizing an Ethical Issue:** Firstly, identify if there is any ethical issue in any given situation and if there are, identify specific ethical aspects of the issue at hand. There are some situations, what appears to be an ethical dispute but is really a dispute about facts or concepts.

**Consider the Parties Involved:** Another important aspect to reflect upon are the various individuals and groups who may be affected by your decision. Consider who might be harmed or who might benefit.

**Gather all the Relevant Information:** Before taking action, gather relevant information, and that all potential sources of information have been consulted.

**Formulate Actions and Consider Alternatives:** Evaluate your decision-making options by asking the following questions:

1. Which action will produce the most-good and do the least harm? (The Utilitarian Approach)
2. Which action respects the rights of all who have a stake in the decision? (The Rights Approach)
3. Which action treats people equally or proportionately? (The Justice Approach)
4. Which action serves the community as a whole, not just some members?   
   (The Common Good Approach)
5. Which action leads me to act as the sort of person I should be? (The Virtue Approach)

**Make a Decision and Consider It:** After examining all of the potential actions, which best addresses the situation? How do I feel about my choice?

**Act:** Many ethical situations are uncomfortable because we can never have all of the information.  Even so, we must often take action.

**Reflect on the Outcome:** What were the results of my decision?  What were the intended and unintended consequences? Would I change anything now that I have seen the consequences?

After the consideration of the guideline for performing ethical decision making, the group did not change their mind about contacting the customers as the decision serves all parties (the store and customers) and not just a selfish act by the store to invade the privacy of the customers. But the following additional information was considered:

**The Ethical Issue:** The ethical issue in the scenario above is privacy; using customer information for another purpose different for the intended use.

**Parties Involved:**

* 1. The grocery store
  2. Customers
  3. Suppliers

**Relevant Information:**

1. Reasons for the contamination
2. Number of customers that purchased the product
3. The ethical implication and the cost
4. Possible legal consequences

**Actions and Consider Alternatives:**

1. Do not use customer information and let the damage occur
2. Do not use customer information but seeks alternatives of reaching the customers such as announcing in social media, TV or radio stations and putting the information on our website
3. Use the customer information and contact them individually.

**Make a Decision and Consider It:**

The grocery store should use the customer information, although it might affect the company’s reputation, but the action produces the most good and do the least harm.

# CIPS code of ethics

This Code establishes guidelines and deals with matters subject to judgment, difficult to state absolutely and which must be judged in light of professional standards in effect at a given time.

## **CIPS imperatives**

### 1. **Protect the Public Interest and Privacy of Information**

CIPS members supposed to carry out their responsibilities with due diligence in regards to the general public in the following ways:

* + Report to the relevant authority problems that might result in serious damage
  + Work in accordance with legitimate rights of 3rd parties, and conduct all activities with due regard for ownership, property rights and privacy.
  + Treat all employer/client business information as confidential, respect copyrights, trade secrets, privacy and terms of license agreements.
  + Give credit where it is due on all reports, papers and ownership of code and designs.
  + Understand and comply with obligations imposed on them under applicable privacy legislation, including The Personal Information Protection and Electronic Documents Act (PIPEDA), and any amendments to or successor legislation.
  + Not discriminate in any manner based on issues such as race, religion, sex, sexual orientation, age, disability, national origin, or social class. Behave as directed regarding any other issue protected by legislation. Exemplify the values of equality, tolerance, and respect for others.

### 2. **Avoid Conflicts of Interest**

Members have the following obligations in regards to Conflicts of Interest:

* + Maintain objective integrity and independence in professional judgment.
  + Not place personal interests or those of colleagues above interests of employers/clients, nor place any interests above those of the public.
  + Make efforts to notify all parties involved and to make full disclosure to the relevant authority if any conflict might be seen to occur by an independent 3rd party.
  + Not enter into reciprocal relationships with third parties who stand to gain as a result of their work.

In a situation of conflict cause by hierarchy of interests, Serving the greater good should be the priority.

### 3. Contribute to the IT Profession

CIPS members have an obligation to take responsibility for results in the following capacities:

* + Achieve and maintain professional competency in their area(s) of practice, as described in the CIPS Common Body of Knowledge.
  + Demonstrate knowledge required to undertake work, be compliant with relevant legislation and accepted standards of practice.
  + Tell the truth and avoid misrepresentation.
  + Balance quality and cost in a very transparent way.
  + Follow policies and client’s code of business conduct, and any contract requirements.

### 4. **Take Professional Responsibility**

CIPS members have an obligation to act in a manner that upholds the reputation of CIPS and the IT profession in general, in relationships with anyone with whom they work; this include making efforts to counter misinformation that could bring the IT profession or CIPS into disregard. All IT professionals are also supposed to support professional development for current and new CIPS members.

## Overview of the CIPS process for decision making

Members should take the following steps when making ethical decisions and resolving ethical dilemmas:

* + Identify the key ethical issues in the situation and what ethical imperatives it relates to
  + Determine what standards of conduct are of major importance to the situation and implement possible actions by:
    - Generating alternatives and examining the risks and benefits of each alternatives
    - Securing additional information
    - Consulting with colleagues, the CIPS Registrar, or with other appropriate sources
    - Examining the probable outcomes of various courses of action
  + Take a moment to reflect on all possible course of actions
  + Determine action plan
  + Take action

In addition, any CIPS member may request interpretation, clarification or amplification of any part of the Code of Ethics (weather general in nature or real situation) this request should be submitted (in confidence) in writing to the Registrar’s Office of CIPS.

After considering the CIPS methodology, it will be necessary to consider the following steps in addition to the guideline for performing ethical decision making discussed earlier. These steps include:

1. Identifying the CIPS ethical imperatives the issue relates to.
2. In considering alternatives, examine the risk and benefits of each of them
3. Consultations with various parities such as colleagues, CIPS Register, or with other appropriate sources.

**References:**

<https://www.ukessays.com/essays/information-technology/the-ethics-and-professionalism-in-information-technology-information-technology-essay.php>

<https://www.quora.com/Why-are-professional-ethics-important>

<https://www.apm.org.uk/blog/the-importance-of-ethics-in-professional-life/>

<https://www.iaa.govt.nz/for-advisers/adviser-tools/ethics-toolkit/professional-ethics-and-codes-of-conduct/>

[**https://www.iuokada.edu.ng/journals/5B6AA29B40ADBA7.pdf**](https://www.iuokada.edu.ng/journals/5B6AA29B40ADBA7.pdf)

<https://geopolicraticus.wordpress.com/2014/09/07/teleological-and-deontological-conceptions-of-civilization/>

<https://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions>

<http://www.cips.ca/ethics>

<https://www.cisco.com/c/en/us/products/security/what-is-it-security.html>

## Case 2: **Ethical Decision Making in Information Technology (A case study of Security Breach)**

**Framework for Ethical Decision Making in Information Technology**

**A case study of Security Breach**

**(COMP 249-001 - Info Security, Privacy and Ethic)**

**By:**

Muhammad Taukirul Islam

Oluwabunmi Olanrewaju

Abimbola Adelegan

Jaden Gerolami

**Consider the scenario**

Data-Time Inc. is a company which manages databases for a large city in Colorado. Included in these databases is information collected from the city’s homeless shelters and free clinics. Specifically, the databases contain personal information of the users of these services over the past 10 years; this includes people’s Social Security numbers and health records.

This data is highly secure and only accessible to the employees of Data-Time Inc. Employees are given a laptop when they are hired which allows them to access the database remotely. Unfortunately, one of these laptops is stolen and the security of the database is compromised.

A majority of the people whose information was compromised are homeless; therefore there is no easy way to contact them in order to alert them of the security breach. How should Data-Time Inc. manage this breach in security?

**Deontological views of Ethics**

Deontological ethics also known as “duty-based” ethics, it states right action consists in following our duty, irrespective of the consequences. It is based on following a set of rules in order to carry out one duty.

The set of rules to be followed in this scenario will be Canada’s *Personal Information Protection and Electronic Documents Act* (“[PIPEDA](http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf)”) as it provides [regulations](http://gazette.gc.ca/rp-pr/p2/2018/2018-04-18/html/sor-dors64-eng.html) relating to mandatory reporting of privacy breaches in Canada.

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information. From the scenario, there was a privacy breach as security of the database was compromised through the stolen laptop. The following steps should be taken to handle the breach:

**Step 1: Reporting the Breach**

* The employee with the stolen laptop should immediately inform his or her immediate supervisor and the information security unit / Privacy Officer of the company.

Once the breach has been confirmed, the privacy Officer will implement the remaining four steps of the breach incident protocol.

**Step 2: Containing the Breach**

The Privacy Officer should take the following steps to limit the scope and effect of the breach:

* Work with units to immediately contain the breach by, for example, recovering the records or shutting down the system that was breached
* Notify the police if the breach involves, or may involve, any criminal activity.

**Step 3: Evaluating the Risks Associated with the Breach**

The following factors will be among those considered in assessing the risks:

* **Personal Information Involved:**
  + What data elements have been breached? The more sensitive the data, the higher the risk. From the case study, Health information, social insurance numbers and financial information that could be used for identity theft are examples of sensitive personal information.
  + What possible use is there for the personal information? Can the information be used for fraudulent or otherwise harmful purposes?
* **Cause and Extent of the Breach:**
  + The cause of the breach (Stolen Laptop).
  + Is there a risk of ongoing or further exposure of the information?
  + What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
  + Is the information encrypted or otherwise not readily accessible?
  + What steps have already been taken to minimize the harm?
* **Individuals Affected by the Breach:**
  + How many individuals are affected by the breach?
  + Who was affected by the breach homeless individuals and those that patronise the free clinics?
* **Foreseeable Harm from the Breach to the individuals**

Harm that may occur includes Security risk (e.g., physical safety), Identity theft or fraud, Loss of business or employment opportunities, negative effects on the credit record, Hurt, humiliation, damage to reputation or relationships or loss of property etc.

* **What harm could result to the Organisation:** Loss of trust in the organisation and litigation.

**Step 4: Notification**

An organization must notify individuals of any breach of the security of safeguards involving their personal information if it is reasonable to believe that the breach creates a “real risk of significant harm.” Concurrently, the organization must also report to the Privacy Commissioner of Canada.

* **Notifying** **Affected Individuals**

1.      Notification to individuals can occur in person when they visit city’s homeless shelters and free clinics

2.      Telephone, mail, email.

3.      Indirect notification - website information or posted notices.

Contents of the notification should include:

* Description of the circumstances of the breach;
* The day or the period during which the breach occurred, or the approximate period;
* A description of the personal information subject to the breach
* A description of the steps taken by the organization to reduce or mitigate the risk of harm from the breach;
* A description of steps individuals can take to reduce the risk of harm that could result from the breach; and
* Contact information that the individual can use to obtain further information about the breach
* **Report to Commissioner**

The report to the Privacy Commissioner must be sent by any secure means of communications and contain the following:

* Description of the circumstances of the breach and the cause, if known;
* The day or the period during which the breach occurred, or the approximate period;
* A description of the personal information subject to the breach, if known;
* The number of individuals or approximate number of individuals affected;
* A description of the steps taken by the organization to reduce or mitigate the risk of harm to affected individuals;
* A description of the steps that the organization has taken or intends to take to notify affected individuals in accordance with PIPEDA; and
* The name and contact information of a person who can answer the Commissioner’s questions on behalf of the organization.

PIPEDA also require organizations to notify additional government institutions if the organization believes that the organization may be able to reduce or mitigate the risk of harm to the affected individuals by issuing the notification.

**Timing of Notifications**

Notification to impacted individuals and the Privacy Commissioner should occur as soon as feasible after the organization determines a breach has occurred.

**Step 5: Record Keeping Requirements**

Most notably, PIPEDA will now require organizations to keep and maintain a record of every breach of security safeguards for twenty-four (24) months. What constitutes a record is subject to interpretation, however, the record must contain any information that enables the Privacy Commissioner to verify compliance with PIPEDA. On request, an organization must be prepared to provide the Privacy Commissioner with access to, or a copy of, a record.

**Teleological views of Ethics**

Teleological ethics, (teleological from Greek *telos*, “end”; *logos*, “science”), theory of morality that derives duty or moral obligation from what is good or desirable as an end to be achieved.

* First, inform your supervisor or boss when you have noticed the stolen laptop. If possible, change password.

**Brown University methodology**

According to Brown University, there are three frameworks for ethical decision making. They are;

**Consequentialist Framework**

This framework focuses on the future effects of the possible course of action, considering people who will be directly or indirectly affected.

**Duty Framework**

Focuses on the duties and obligations that we have in a given situation and consider what are the ethical obligations we have and what things we should never do.

**Virtue Framework**

This framework identifies the character traits (either positive or negative) that might motivate us in a given situation. We are concerned with what kind of person we should be and what our actions indicate about our character. We define ethical behavior as whatever a virtuous person would do in the situation, and we seek to develop similar virtues.

The management of Data-Time Inc. needs to apply the following processes on making ethical decisions for the case at hand:

**Recognizing an Ethical Issue**

* How can we limit the impact of privacy breach?
* What impact will this theft have on affected individuals?
* How does this affect company reputation and brand?
* Is there a way to have prevented this exposure from occurring?
* Is there a way to forestall recurrence?

**Consider the Parties Involved**

* Decision makers at Data-Time Inc.
* Data-Time IT department
* Privacy commissioner office
* E-Health Canada
* Police
* Management and employees of homeless shelters and free clinics.
* Homeless people involved (we assume Data-Time has back-up information on a server)
* Next of kin of homeless people
* Other individuals who are not homeless (these can be contacted directly)

**Gather all the Relevant Information**

* Get contact details of those reachable
* Data-Time has information on affected citizens on other connected computers and server
* Can the stolen laptop be remotely programmed to self-destruct any stored information?
* Make a list of people involved

**Formulate Actions and Consider Alternatives by asking the following questions:**

*Which action will produce the most good and do the least harm? (****The Utilitarian Approach****)*

* Put up signs at shelters and clinics about the possible breach
* Get the information out on local and social media

*Which action respects the rights of all who have a stake in the decision? (****The Rights Approach****)*

* Inform the Privacy Commissioners office and law enforcement
* Contact those who could be reached

*Which action treats people equally or proportionally? (****The Justice Approach****)*

* Public announcement
* Contact affected individuals and inform the next-of-kins of those we don’t have contact information on

*Which action serves the community as a whole, not just some members?* ***(The Common Good Approach)***

No single action serves the entire stakeholders. A collection of actions is involved, such as;

* Investigate the theft and build stronger data handling protocol
* Make sure computers containing such sensitive information are better-protected and secured onsite.

*Which action leads me to act as the sort of person I should be? (The Virtue Approach)*

* Report to appropriate authorities and don’t attempt a cover-up

**Make a Decision and Consider It**

After examining all of the potential actions, which best addresses the situation? How do I feel about my choice?

* The **Common group approach** may be the best in this situation, so that we can reduce the risk of future recurrence by domiciling such sensitive information to a secure onsite server.
* Cooperate with law enforcement agents to make sure the employee whose laptop was reported stolen had no malicious intent

**Act**

Many ethical situations are uncomfortable because we can never have all of the information.  Even so, we must often act.

* Report to Police and Privacy Commission
* Revise remote access rights of employees
* Notify the public of the incident
* Adhere to recommendations of privacy office

**Reflect on the Outcome**

What were the results of my decision?  What were the intended and unintended consequences? Would I change anything now that I have seen the consequences?

**Intended Consequences:**

* People who potentially got their private information exposed are aware of the issue.
* Words will get out that the firm was involved in data security breach

**Unintended Consequences:**

* Reputation damage
* Possible negative backlash from the public
* Cost of conducting damage control

**CIPS code of ethics**

**The Four CIPS Imperatives**

Distinguishing marks of a profession are its acceptance by the public, and the profession's acceptance of its responsibility to the public. The following statements are a set of high ideals to which all CIPS members aspire. CIPS members have an obligation to:

**Imperative #1: Protect the Public Interest and Privacy of Information**

* Carry out work or study with primary regard for public interest (including health, security, safety, privacy, protection of the environment and social responsibility) and in accordance with regulatory requirements and legislation.
* Report to the relevant authority the breach in security such as Privacy Officer of the company and police

**Imperative #2: Avoid Conflicts of Interest**

Act so the welfare of others takes precedence over personal interests and provide full disclosure to impairment of personal judgment.

**Imperative #3: Take Professional Responsibility**

Serve their employer/clients competently, carry out their work with due diligence, maintain and advance their knowledge and exercise uncompromised professional judgment.

**Imperative #4: Contribute to the IT Profession**

Respect the rights and professional aspirations of colleagues and uphold the integrity, dignity and image of the profession.

**The CIPS Process of Ethical Decision-Making**

Members should take the following steps when making ethical decisions and resolving ethical dilemmas:

* Identify the key ethical issues in the situation: **Security Breach**
* Identify what ethical imperatives are relevant to the situation: **Imperative 1**
* Determine what standards of conduct are of major importance to the situation and begin to implement some possible actions by:
  + generating alternatives and examining the risks and benefits of each
  + securing additional information
  + consulting with colleagues, the CIPS Registrar, or with other appropriate sources
  + examining the probable outcomes of various courses of action
* Take a moment to reflect. (Include in the decision-making process the feelings and intuitions evoked by the ethical challenges. You might decide that you would feel uncomfortable with certain alternatives even if the action can be justified)
* Determine action plan
* Take action (follow a concrete action plan, evaluate the plan, and be prepared to correct any negative consequences that might occur from the action taken).  Such requests may be general in nature or may refer to a particular hypothetical or real situation or be submitted (in confidence) in writing to the Registrar’s Office of CIPS.

In addition, any CIPS member may request interpretation, clarification or amplification of any part of the Code of Ethics.

**Case reflection**

The CIPS Methodology would result in additional steps that was not considered previously. The additional steps would include

* Identify the key ethical issues in the situation
* consulting with colleagues, the CIPS Registrar, or with other appropriate sources
* examining the probable outcomes of various courses of action
* Formulation of more concrete written action plan

So the following steps can be useful for Data-Time Inc to secure their data and privacy according to CIPS code of ethics

* **Conduct a Risk Assessment**

The risk assessment forces providers to review security policies, identify threats and uncover vulnerabilities within the system. Data-Time Inc. should conduct a routine maintenance and risk assessment including security patches, operating system upgrades etc.

* **Provide Continued Education to Employees**

Educate and re-educate employees on data security can significantly reduced data breaches, so Data-Time inc should arrange proper training for employees.

* **Monitor Devices and Records**

Remind employees to be watchful of electronic devices left unattended. More often than not data breaches occur due to theft of these items from a home, office or vehicle. While it is IT’s job to safeguard patient information, employees should be reminded to do their part in keeping data safe as well. Make sure to always lock your device whether it’s a laptop, desktop, or phone and password protect it.

* **Encrypt Data & Hardware**

Encryption technology is key in avoiding data breaches. so Data-Time Inc should encrypt their data on regular basis which can prevent data breaches.

* **Developing a secure way of accessing data remotely**

Data-Time Inc can develop a system so employees will be able to access data remotely from server instead of taking device outside the office which will be convenient for both employees as well as company.

Following these additional steps would result a more comprehensive solution to decide. By identifying the key ethical issues of the situation and consulting with colleagues, the CIPS Registrar, or with other appropriate sources would help to get additional insight into the matter. Examining the probable outcomes of action and preparing concrete written action plan would help Data-Time Inc to follow proper ethical procedure.

**Group Decision**

What course of action would your group recommend in this case?

* The **Common group approach** may be the best in this situation, so that we can reduce the risk of future recurrence by domiciling such sensitive information to a secure onsite server.
* Cooperate with law enforcement agents to make sure the employee whose laptop was reported stolen had no malicious intent
* Remotely wipe the OS or contents of the stolen laptop so that whoever has access to the physical laptop cannot access the database
* Seek advice from CIPS or privacy office on how to go about resolving the breach

**References**

1. “Brown University.” *Decameron Web | Society*, Brown University, [www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions](http://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions).
2. <https://www.cyberadviserblog.com/2018/09/mandatory-data-breach-notification-in-canada-understanding-your-new-obligations/>
3. <https://www.mun.ca/iap/privacy/Managing_a_Privacy_Breach0526.pdf>
4. <http://www.cips.ca/sites/default/files/CIPS%20Code%20of%20Ethics%20and%20Standards%20of%20Conduct%20-%20June%202018.pdf>
5. <https://www.britannica.com/topic/teleological-ethics>

# Speaker Reflection

## Speaker 1: Matthew Vaughan /SGI

# Guest Speaker: SGI

# The Guest: SGI

Speakers: Matthew Vaughan

## Overview:

What were the major themes pf the presentation?

* Working in public sector
* Differences between public sector and private sector such as
  + Quick to change in private sector
  + Potential for higher reward in private sector
  + Non-Union in private sector
  + More control over career
  + While there is lots of training opportunities in public sector
* Six important things to know:
  + You control your career
  + Interviewing takes practice
  + Embrace the change
  + Build meaningful relationships
  + Communication is key
  + Find your thing

Identify the most interesting part of the presentation.

* Six important things to know:

What did you learn from the presentation?

How to implement change in a rigid environment without breaking the law and always taking accountability for your action.

## Discussion:

Did you ask any questions? If so what? Summarize the answer. No

What did others ask? Summarize the answer. What employers wants in new intakes?

To show initiatives

## Feedback:

Do you have any feedback for this presenter? No

## Speaker 2: Todd Anthill / Nutrien

The Guest: **Nutrien, VP IT**

Speakers: Todd Anthill

## Overview:

What were the major themes pf the presentation?

* About Nutrien:

They are into production and distribution of [potash](https://www.nutrien.com/what-we-do/our-business/potash), nitrogen and [phosphate](https://www.nutrien.com/what-we-do/our-business/phosphate) products for agricultural, industrial and feed customers world-wide.  Currently, they are the largest potash producer in the world. They also operate a leading agriculture retail network that services over 500,000 growers.

* Innovative Technology the organization is undertaken
* Their Underground mining operations
* Personal discovery

Identify the most interesting part of the presentation.

Todd talked about being a self-starter irrespective of the organization and ability to grow your career

What did you learn from the presentation?

The ability to put your career into your won’s hand.

## Discussion:

Did you ask any questions? If so what? Summarize the answer. No

What did others ask? Summarize the answer.

## Feedback:

Do you have any feedback for this presenter? No

\* A minimum of 2 feedback emails are required for the appendices of your reflection portfolio

## Speaker 3: **2nd Year BIS Volunteers** / COOP Student Panel

The Guest: **2nd Year BIS Volunteers**

Speakers: Graham, Jake, Parth, Brad, Junaid, Maulik, Justin

## Overview:

What were the major themes pf the presentation?

* Various places each of them did their coop
* Experiences obtained during the period
* Advise to us as we look forward to start our coop

Identify the most interesting part of the presentation.

* Advise to us as we look forward to start our coop

What did you learn from the presentation?

The pay should not be the paramount factors in considering a coop work term as there are some organizations not offering much but one can learn lots on the job.

## Discussion:

Did you ask any questions? If so what? Summarize the answer. Yes

I asked about accommodation and the answer was it depends on the organization.

What did others ask? Summarize the answer.

* The technology use on the job; this include ASP.Net, VDI etc.

## Feedback:

Do you have any feedback for this presenter? yes

\* A minimum of 2 feedback emails are required for the appendices of your reflection portfolio

## Speaker 4: Mark Plosz / Paradigm Consulting

The Guest: <http://www.paradigm-seb.com/>

Speakers: Mark Plosz (VP, Application and Technology Services)

## Overview:

What were the major themes of the presentation?

* Who they are and what they do: Paradigm provide management consulting, change management and application and IT services to corporate and government clients. There clients are in both private and Public Sector
* People in Paradigm: Paradigm people are employed from various age and race as so on you have something to contribute
* Projects in paradigm: They undertake different projects from various sectors making employees knowledgeable in various areas, and as a result they have to be ahead of the game in terms of the next level in IT

Identify the most interesting part of the presentation.

* The part where he talked about their people, the various opportunities in paradigm and the ability to grow as an employee in the company as so on you are innovative, and you have the ability to take your career into your hands.

What did you learn from the presentation?

* The various opportunities in IT, some exams you can take if one wants to specialize in a particular area and how it is necessary to keep learning if one wants to remain relevant and advance his/her career.

## Discussion:

Did you ask any questions? No

What did others ask? Questions on careers including coop work, technology used, paradigm next move etc.

On career, he said he still talking to Trudy on coop but anyone interested to work with them can apply online.

## Feedback:

Do you have any feedback for this presenter? Yes

# Appendices

## Appendix A. Ethical Decision Making Framework

* CIPS Code of Ethics and Standards of Conduct
* brown.edu Framework for Making Ethical Decisions

please check the attached folders for this documents.

## Appendix B. Speaker Feedback Emails



